Notes for 3rd Jan (Thursday)

1 The road so far...

1. Stated the Axiom of Choice.
2. Defined equivalence relations, gave examples, and proved the link with partitions.
3. Defined involutions, stated a lemma, and proved Fermat's theorem on squares.

2 Partial orders

We now want to define an order $\leq$ on the natural numbers, and more generally, on other sets. A partial order $\leq$ on a set P (such a set is called a poset) is a relation such that it is

1. Reflexive : $x \leq x \ \forall \ x \in P$.
2. Transitive : $x \leq y, y \leq z \Rightarrow x \leq z$.
3. Antisymmetric : $x \leq y, y \leq x \Rightarrow x = y$.

If for any two elements x, y either $x \leq y$ or $y \leq x$, then the partial order is said to be a total order (a totally ordered set is called a chain).

Here are examples and counterexamples :

1. Equality is a total order.
2. The "usual" order on $\mathbb{N}$ (defined inductively) is a total order. In fact, it is even better. Every non-empty subset has a least element. Such an order is called a well order. The well-ordering principle (equivalent to the axiom of choice) says that every set has a well order !! This makes it possible to apply some kind of induction (transfinite induction) to prove theorems on arbitrary sets.
3. The set of subsets of X has a partial order given by inclusion. This partial order is not a total order.
4. The set of events in special relativity ordered by causality.

The point of defining partial ordering is Zorn's lemma.

Theorem 1. *The axiom of choice is equivalent to the following statement : In a partially ordered set* $(S, \leq)$*, every chain that has an upper bound has a maximal element, i.e., an element* M *such that if* $x \geq M$ *then* $x = M$*. (Note that in the poset* $a_1 < b_1 > a_2 < b_2 \ldots$*, all the* b_i *are maximal elements.)*

As Jerry Bona said, "The Axiom of Choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn's lemma?" Zorn's lemma can be used to prove many things like "Every vector space has a basis" and "There exists a maximal Globally Hyperbolic Caucy development in General Relativity !"

3 Cardinality

The cardinality of a finite set A is intuitively speaking, the number of elements of A. For infinite sets, obviously this notion does not make sense. However, one can still ask if two infinities are the same (!) in the following manner.
Two sets A and B are said to have the *same* cardinality if there exists a bijection from A to B.
We define a set to be finite and having cardinality n if it is in bijection with $\{1 \leq i \leq n\}$. You might think that it is circular because at the very foundation of mathematics we assumed the notions of "finite" (as in finite alphabet for instance). However we are talking about "finite sets" here (treat it as a single noun if it makes more sense to you). This is the only way to define the notion.
One can prove that set of natural numbers is infinite. Indeed if it is in bijection with $\{1 \leq i \leq n\}$ then natural numbers would have to be bounded (because if not, then there are more than n natural numbers and finite cardinality can be easily proven to be unique). But this is a contradiction by Peano's axiom ("no ceiling" axiom).
However infinite sets are weird. Define a number to be even if $n = 2k$ and odd if $n = 2k + 1$.
Firstly, every number is definitely either even or odd but not both. This follows from the Euclidean algorithm. Also, the k is unique given n.
Secondly, the set of even numbers is in bijection with natural numbers despite being contained in it. Indeed, map an even number $n = 2k$ to the corresponding k. This is a well-defined function. It is an injection because if $2k = 2l$ then by the cancellation law $k = l$. It is a surjection too. Likewise, positive naturals have the same cardinality as naturals. Any set that has the cardinality of naturals is said to be countably infinite.
Here is a fundamental result.

Theorem 2. *There is no surjection from* X *to its power set* $\mathcal{P}(X)$*, i.e., the power set has strictly "larger" cardinality.*

Proof. The following proof is due to Georg Cantor. He introduced a revolutionary idea of a proof, now called "Cantor's diagonalisation". Cantor was branded a charlatan (by Kronecker) and his ideas "a disease" by Herni Poincaré. Cantor has been well vindicated.
Suppose there is a surjection $f : X \to \mathcal{P}(X)$. Then consider the subset of X given by $A = \{a \in X | a \notin f(a)\}$. This we claim cannot be in the image of f thus producing a contradiction. Indeed, if $f(b) = A$, then there are two possibilities. Either $b \in f(b)$ which

means it cannot be in $f(b)$, or $b \notin f(b)$ which means it has to be in $f(b)$ (the barber paradox). $\square$